FISMA Compliance:
Making the Grade

A Qualys Guide to Measuring Risk, Enforcing Policies, and Complying with Regulations

EXECUTIVE SUMMARY

For federal managers of information technology, FISMA is one of the most challenging pieces of federal legislation to be enacted in recent years. On the one hand, FISMA imposes strong requirements to rapidly improve the security of government information, and it holds agencies fully accountable for their success in meeting this goal. On the other hand, for managers who can meet those requirements, there are new opportunities to refocus resources within security programs and to obtain tools to manage them adequately. As discussed in this White Paper, QualysGuard can help agencies meet FISMA requirements, reduce the cost of compliance, and use industry best practices to meet FISMA challenges head-on.

FISMA Defined

Formally titled “The Federal Information Security Management Act of 2002”, FISMA is part of the E-Government Act of the same year. FISMA’s provisions fall into three major categories: assessment, enforcement, and compliance. The first pertains to determining the adequacy of the security of federal assets, the second requires that key information security provisions be implemented and managed, and the third establishes provisions for the management of each agency’s information security program and the accountability of each agency for compliance and reporting.

QualysGuard Supports FISMA Compliance

To be successful in meeting FISMA requirements, federal agencies need automated tools to help them manage their security programs, perform continuous system assessments, support accurate reporting on compliance activities, and enable measurements of how well they are meeting all of FISMA’s provisions. QualysGuard is the ideal tool for this purpose.

Requiring no software to install or maintain, QualysGuard automates security audits, providing strong protection against the myriad of threats to federal agency technology. This Paper describes key provisions of FISMA and shows how QualysGuard supports compliance by enabling federal IT managers to collect, manage, and report on accurate information about their enterprise security posture.

QUALYSGUARD ASSESSES SECURITY

Recognizing that “what cannot be measured cannot be improved,” FISMA requires that agencies maintain an inventory of major information systems and a set of baseline system configuration requirements. Agencies must undertake regular security assessments with clear plans of action for correcting any issues found, and must handle security incidents as they are found.

Inventory

QualysGuard inventories the agency’s network-attached hosts and IP devices through a series of advanced discovery techniques. During Certification and Accreditation, each system’s assets can be identified and grouped together in various ways, such as by organization, operating system or network location. Most important for FISMA, QualysGuard maps the relationships between assets to help assign accountability and system ownership for inventoried assets.

System Configuration

Additional system configuration reports show more specific features, such as operating system, protocols and services present on each inventoried item. Vulnerabilities are identified by asset, allowing audits to be targeted as appropriate and enabling quick decisions about where to focus mitigation activity.

Assessments

Vulnerability assessments can be configured in a number of effective ways, including using scans input to risk assessments, displaying the likelihood and potential impact of exploitation, and mapping changes to the existence of vulnerabilities over time.

Incident Handling and Response

QualysGuard scans give an early warning of organizational exposure to new vulnerabilities, so that incidents are prevented before they even occur. Reports recommend mitigation techniques, including links to vendor web sites for downloading patches and other remedial resources. This feature fosters a unified organizational approach to potential incidents. It ensures that all system administrators have access to the same tool sets, the same knowledge about how to correct vulnerabilities and a common framework for response.

FISMA Requires Agencies to:

1. **ASSESS** Measure the agency’s security posture.
2. **ENFORCE** Ensure that security requirements are met.
3. **COMPLY** Assign accountability for results.

See the full text of FISMA at csrc.nist.gov/policies/FISMA-final.pdf

Government Scorecard

““One of the most disturbing findings is that 19 of the 24 agencies reviewed had not completed an inventory of their mission critical systems. Obviously, an agency can’t ensure its systems are secure if it can’t account for all of its mission critical systems. Everything starts with the inventory, and this aspect must improve -- and improve quickly.”

Gov’t Reform Subcommittee on Technology Information Policy, Intergovernmental Relations and the Census

Chmn. Adam H. Putnam (R-FL)
Remarks concerning the 2003 Federal Computer Security Report Card

QUALYSGUARD SUPPORTS ENFORCEMENT

> *"Each Federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…"*
>
> **The Federal Information Security Management Act of 2002, §3544**

FISMA requires the reporting of significant deficiencies. Agencies must identify and track material weaknesses, reporting progress on corrective action quarterly. Using a Plan of Action and Milestones (POA&M), each agency must commit to a schedule of remediation and is held accountable for completing each corrective task. The agency's success in undertaking corrective action and in improving compliance is tied directly to its requests for funding and to the budgets that are allocated for IT programs and systems.

Related Legislations

Homeland Security Presidential Directive #7 – (Critical Infrastructure Identification, Prioritization, and Protection)

OMB Circular A-130 Appendix III – (Security of Federal Automated Information Resources)

Management Accountability

A fundamental new requirement imposed by FISMA is increased accountability of agencies and officials. QualysGuard addresses this requirement with a robust set of management reports showing the security status of assets owned by each organization and manager. This information documents accountability for enforcement in each agency for each person with authority for management of each asset. Reports can be configured to show a static moment in time or to view trends across time.

Determination of Risk

FISMA reinforces existing federal requirements to determine agency risk by mandating that agencies meet security objectives "commensurate with the risk and magnitude of the harm" inherent in that risk. QualysGuard reports identify the specific level of risk for each vulnerability identified in the network. In the next product release, system administrators and managers will be able to create user-defined risk levels, a particularly important feature for agencies with unique or self-defined assessment methodologies.

Mitigation and Tracking

Given FISMA's focus on measurement, enforcement and compliance, it is critical for agency managers to be able to track significant deficiencies and the remediation actions taken to correct them. With QualysGuard, system administrators can filter reports to show specific vulnerabilities and their recommended corrective measures. Trouble tickets can be assigned to appropriate personnel to enforce remediation requirements, and to ensure that enforcement is handled consistently across the agency. QualysGuard reports demonstrate the exact status of all mitigation activity. Items that have been corrected can be highlighted; vulnerabilities that are still active can be referred for follow-up activity.

QUALYSGUARD MEASURES COMPLIANCE

FISMA introduces significant new requirements for regular reporting of information security program progress and results. With QualysGuard, FISMA compliance and reporting information is readily available at a moment’s notice, including reports on the status of Certification and Accreditation tasks, ongoing monitoring of application systems, and updates on the status of the Plan of Action and Milestones activities.

Reporting

Management and technical reports can be produced to show any view of the enterprise, at any level of detail. Management can focus on particular vulnerabilities to quickly correct “hot” issues, such as exposures to the SANS Top 20 list of vulnerabilities. Trend information shows the history of the security program over time, including key changes to the level of threats and vulnerabilities.

Strategic Planning

FISMA provides for the full integration of information security management processes with strategic and operational planning. To ensure that each agency complies with FISMA’s provisions, the Act requires that the success of the security program be highlighted in agency performance and financial planning reports.

QualysGuard reports can help with the integration process. High-level reports showing overall status of security and asset management can be included in Exhibits 53 and 300B input to capital planning process. Improvements to security can be measured and used to support program management and operational planning activity.

Training

Agencies must have policies and procedures that support compliance and training for key ISS personnel. QualysGuard scan output and reports can show where policies and procedures need to be strengthened by highlighting trends where response was inadequate or where issues arose during remediation activity. Agency management can use these reports to assess staff response to vulnerabilities and determine requirements for additional training. Finally, QualysGuard contains many built-in training features, such as those that link to web sites with further information about risks and vulnerabilities, and how to correct security issues.

SUMMARY OF QUALYSGUARD'S FISMA CAPABILITIES

The table below provides a quick-reference view of how specific FISMA provisions are supported by QualysGuard's features, functions and capabilities.

FISMA Requirement	QualysGuard Capability
Specific **accountability** of agencies and officials	Regular reports show security status of assets owned by each organization and manager
	Summary reports show enterprise view for formal FISMA reporting
Assess **risk** by seeking to meet defined security objectives	Reports provide identification of levels of risk, including user-defined levels in next release
	Data can be used in risk assessments to support Certification and Authorization activity
	Managers can make risk-based decisions about asset management
Maintain an **inventory** of major systems and interconnections	Tool can be used to uncover all assets in defined domain, including those previously "undiscovered", to build and maintain the inventory
	Relationships between assets can be mapped to help assign accountability for inventoried assets
Regular security **assessments** and reviews	Vulnerabilities are identified by asset, allowing audits to be targeted as appropriate
	Scans can be run and used as input to assessments
	Assessments are automated, reducing staffing costs, and include identification of likelihood and impact assist with Certification and Accreditation activity.
	Changes can be mapped over time to audit compliance with recommendations in earlier assessments
Significant regular **reporting** of ISS program progress and results	Trend information includes changes to level of threats and vulnerabilities
	Management can focus on particular vulnerabilities to quickly correct "hot" issues, such as SANS Top 20
	Reports can list corrected vs. still active vulnerabilities to show status of corrective action
	Data can be summarized to provide each level of management with their own view of security "health"
Tracking of significant deficiencies and **remediation** actions taken	System administrators can filter reports to show specific vulnerabilities and recommended corrective measures
	Trouble tickets can be assigned to appropriate personnel to enforce remediation requirements
	Reports show exact status of mitigation activity - corrected vs. still active vulnerabilities
Incident response and prevention processes and capability	Scans give early warning of organizational exposure to new vulnerabilities
	Recommended mitigation actions foster unified organizational approach to potential incidents
	Specific vulnerabilities are mapped to assets for more rapid assessments and response
	Reports can be shared with internal and external incident response organizations

FISMA Requirement	QualysGuard Capability
Compliance with minimum system **configuration** requirements	Reports identify asset features and components such as OS, protocols and services
	The mapping of specific vulnerabilities to assets shows compliance with configuration management requirements
Policies and procedures which support **compliance and training** for key ISS personnel	Scan output and reports show where policies and procedures need to be strengthened
	ISS staff response to vulnerabilities can be assessed to determine where training is needed
Integration of security management processes with strategic and operational planning	High-level reports showing overall status of security and asset management can be included in Exhibits 53 and 300B input to capital planning process
	Improvements to security can be measured and used to support program management and operational planning activity

References

1. Federal Information Security Management Act (FISMA, P.L. 107-347, Title III); December 17, 2002 http://www.csrc.nist.gov/policies/FISMA-final.pdf
2. OMB Memorandum 03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting, August 6, 2003. http://www.whitehouse.gov/omb/memoranda/m03-19.pdf
3. The New FISMA Standards and Guidelines, Changing the Dynamic of Information Security for the Federal Government, Dr. Ron S. Ross, Computer Security Division, National Institute of Standards and Technology, posted at http://csrc.nist.gov/sec-cert/fisma-article-v15.pdf
4. Executive Order: Critical Infrastructure Protection in the Information Age, http://csrc.nist.gov/policies/cip-infoage.html

CONCLUSION

According to NIST, “Achieving adequate, cost-effective information system security….in an era where information technology is a commodity requires some fundamental changes in how the protection problem is addressed. [1]Because FISMA compliance is tied to program funding, agencies that do not meet its requirements risk losing critical program and system resources. However, in many agencies, the issue is not becoming compliant, but in managing the data that proves compliance. Sifting through mountains of data can be a daunting task, since it often must be done manually, with risk of errors.

QualysGuard makes it possible to demonstrate compliance and to support funding requests without the need to dig into the underlying details. With a few clicks of a mouse, reports can be configured to show the exact status of the agency’s security posture, the history of corrective action, the timing of response to incidents, and literally thousands of other statistics that contribute to FISMA compliance reporting.

QualysGuard can help create a consistent, enterprise-wide view of each agency’s security posture, creating ties between program activities such as assessment and remediation and showing managers at all organizational levels exactly where they stand in addressing security issues. Even when key program components to support FISMA are missing, QualysGuard fills in the gaps. By allowing for collection of a complete inventory, creation and enforcement of configuration management standards, and identification of risks to all inventoried assets, QualysGuard creates a unified, agency-wide, FISMA-compliant view of the state of the agency’s security health.

In short, WITHOUT QualysGuard, agencies may be non-compliant with FISMA’s provisions, and at risk for further security issues. WITH QualysGuard, agencies can quickly see where they stand, correct those issues, and move forward with confidence towards a robust, well-managed security program.

[1] The New FISMA Standards and Guidelines

ABOUT QUALYS, INC.

Qualys is the market-leading Web Service Provider offering on-demand Network Security Audits and Vulnerability Management. Qualys enables large and small organizations to manage security from an attacker's perspective and fix real-world weaknesses before they are exploited. Qualys' web services are used simultaneously by executives and technicians to measure security effectiveness, enforce security policy, and comply with regulations. Thousands of customers rely on Qualys, including Hershey Foods, Hewlett Packard, and The Thomson Corporation. Qualys is headquartered in Redwood Shores, California, with global offices in France, Germany and the U.K.

Qualys, Inc.
1600 Bridge Parkway
Redwood Shores, CA 94065
1 (800) 745 4355
www.qualys.com